International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183862

Emerging Cyber-Physical Systems : An Overview

Okolie S.O., Kuyoro S.O., Ohwo O. B

Department of Computer Science, Babcock University, Ikenne, Nigeria

ABSTRACT

Cyber-Physical Systems (CPS) will revolutionize how humans relate with the physical world around us. Many grand challenges await the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defence, aerospace and buildings. Exploration of these potentialities around space and time would create applications which would affect societal and economic benefit. This paper looks into the concept of emerging Cyber-Physical system, applications and security issues in sustaining development in various economic sectors; outlining a set of strategic Research and Development opportunities that should be accosted, so as to allow upgraded CPS to attain their potential and provide a wide range of societal advantages in the future.

Keywords : Cyber-Physical Systems, Transportation, Health-Care, Manufacturing, Agriculture, Energy, Defence, Aerospace

I. INTRODUCTION

Cyber-physical systems (CPS) are physical and engineering systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. The Nano-world to large-scale wide-area systems of systems would display the close arrangement between the cyber and physical (Ragunathan, Insup, Lui, & John, 2010). The web changed how people connect and speak with each other, upset how and where data is gotten, and even changed how individuals purchase and offer items. Likewise, CPS will change how people communicate with and control the physical world around us.

Use cases of CPS incorporate medical devices and systems, aviation systems, transportation vehicles and smart expressways, mechanical frameworks, process control, industrial facility automation, building and natural control and smart spaces. CPS cooperate with the physical world, and must work reliably, securely, safely, and effectively and progressively.

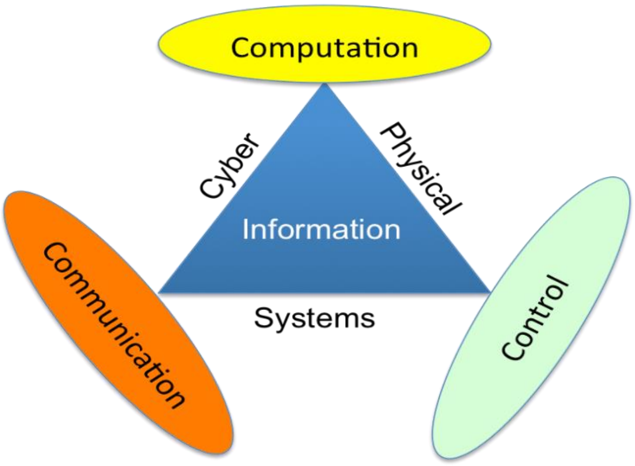

Figure 1 : Cyber-Physical System Overview
Source: (Erik, 2018)

The growth of low- cost and high capability sensors which possess tiny look, the increasing accessibility of higher powered, high- capability, tiny computing devices; all these factors have contributed to the guarantee of CPS. The requirement for CPS innovations is additionally being handled by CPS sellers in areas like aviation, engineering and environmental control, smart grid, process control, manufacturing plant automation, and medical services, who are progressively finding that the innovation base to fabricate huge scale safety-critical CPS effectively, moderately, adaptably and on plan is genuinely deficient. CPS unite the distinct and potent logic of computing to admonish and operate the persistent elements of physical and engineering systems (Ragunathan, Insup, Lui, & John, 2010).

The future utilizations of CPS are more transformative than the Information Technology of the previous three decades. Unparalleled expository capacities, real-time networked information, and pervasive sensing, actuating, and computation are making intense open doors for systems integration. Cutting edge CPS will have the capacity to execute phenomenal errands that are scarcely envisioned today. These new abilities will require high-certainty processing frameworks that can associate fittingly with people and the physical world in unique situations and under unexpected conditions. The advancement and improvement of CPS would need computer scientists, researchers and system experts to experiment with specialists in different engineering fields such as control engineering, signal processing, civil engineering, mechanical engineering and biology. Thus, this will upset how institutions educate scientists and engineers. The size, organization and capabilities of industry groups that design, develop and deploy CPS will likewise change significantly. The worldwide intensity of national economies that progress toward becoming innovation pioneers in CPS will make strides (PCAST P. C., 2007).

The exactness of computing must interface with the vulnerability and the commotion in the physical environment. The absence of ideal synchrony crosswise over time and space must be managed. The disappointments of parts in both the digital and physical areas must be endured or tolerated. Security and privacy prerequisites must be implemented. System elements over numerous time-scales must be tended to. Scale and expanding many-sided quality must be subdued. These requirements require the production of innovative scientific foundations and engineering principles. Experimenting ways to deal with assembling computing-centric engineered systems must be supplanted by thorough strategies, confirmed frameworks, and capable devices. Investigations and science must supplant wasteful and testing-concentrated strategies. Startling mischances and disappointments must blur, and strong system configuration must turn into a set up area. New sensors and sensor combination innovations must be created. Smaller and all the more intense actuators must wind up plainly accessible (Ragunathan, Insup, Lui, & John, 2010).

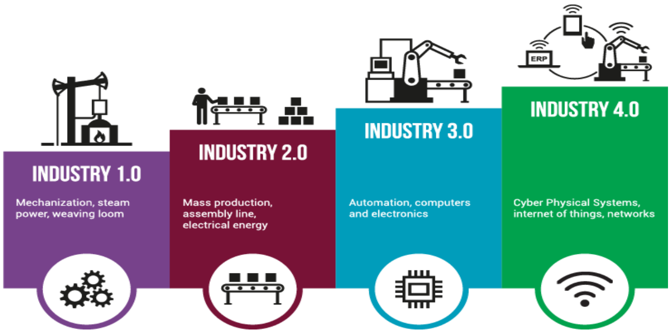
INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
ERP

Figure 2 : Evolution to Cyber-Physical Systems (Industry 4.0)

Source: (Jay, 2018)

II. LITERATURE REVIEW

The literature review features some safety efforts that have been proposed and utilized in the progression of Cyber Physical System in different fields of uses and in addition instruments for the confirmation and approval of Cyber Physical Systems.

(Insup, et al., 2012), thought about Medical CPS as an unquestionable CPS space. In light of extending societal pressures and new inventive abilities, the field of Medical CPS is practically a significant change that will change the manners in which these frameworks are made and confirmed, and furthermore develop and strengthen safety ensures the Medical CPS offer to workers and patients. For the plan of a safe physiological close-circle framework, the iterative check and approval approach was pursued. To begin with, recognize solid utilize cases, at that point demonstrate singular parts of the framework: the patient, observing and conveyance gadgets, and system. The patient model is created by executing physiological models on confirmation and reproduction apparatuses, for instance, UPPAAL and Simulink. By considering the estimation and movement, mistakes that sensible gadget may show, the information yield conduct of observing and conveyance gadgets was displayed. The system display portrays the factual conduct of system correspondence. Next, the entire course of action of a controller was demonstrated and planned by associating and characterizing interfaces between particular parts. By then a risk examination was performed and possible explanations behind each hazard was recognized. Such disillusionment conditions were effectively perceived and checked whether all security properties are satisfied in all circumstances, by running reproduction on Simulink and formal confirmation on UPPAAL. The controller and framework plans were rethought until the point when the moment that all dangers are wound up being truly directed. Check of physiological shut circle frameworks remains a significant test. In the end, clinical outcomes passed on by a shut circle framework ought to be appeared differently in relation to current parental figure driven methodologies. Examining the usage of SimMan, which gives a controlled, reasonable providing care condition with patient test system. Similarly, the piece of a parental figure in a shut circle framework ought to be viewed as even more purposely. Everything considered, we are not going for totally independent frameworks that avoid people.

(Shailesh, 2014), exhibited how we can execute Medical CPS in perspective of detecting and observing framework the dynamic occasion. The structure state contains two sorts of information examination: one is movement investigation and second flag examination. In the midst of movement examination, the body development of patient are caught and are used for the investigation of the patient conduct. In the midst of flag investigation, the gotten signs from sensor are broken down. The engineering involves three level of information handling. The level 1 uses the diverse calculation with the end goal to recognize the occasion. Level 2 apply rule base model at this level the choice is gone up against premise of characterized rule. Level 3 has a most noteworthy cognizance in the framework, at this level framework produce finish familiarity with the physical world. By the use of the proposed engineering the expense of handling can be diminished. Nevertheless, the proposed framework ought to be attempted on the constant situation.

(Shah, Syed, and Mustafizur, 2014), evaluated CPS in human services and given a compact audit of CPS. By then a depiction (mapping) of CPSs for social insurance applications dependent on a broad logical arrangement including eight substitute perspectives (or parts): application, designing, recognizing, data organization, figuring, correspondence, security, and control/initiation. This depiction was helpful in imagining the examples, frameworks, and potential CPS arrangements around particular applications. The mapping of the logical arrangement to CPS ventures has also included therapeutic administrations solely utilizing Wireless Sensor Networks (WSN) or Cloud Computing. Consequently, the logical arrangement and the mapping showed in this paper can in this way be used to recognize the holes between WSN or cloud-based human services arrangements and CPS based arrangements. Security and protection issues were recognized as the scarcest examined in CPS for social insurance applications.

(Tianbo, Jinyang, Lingling, Yang, and Xiaoyan, 2015), gave a broad survey on CPS security following the security framework from different perspectives. With the growing transcendent utilize and vulnerabilities of CPS to digital physical assaults. A survey among the primary universities and establishments driving the investigation of CPS security was performed and separated fixation on the relations between them. The goals for achieving security of CPS in different perspectives were given related composition tries. By then the crucial security approaches on perceiving digital physical assaults and ensuring CPS security are recorded and examined. At long last, a summary of security in particular applications with the predominant research bunch was shown. In like manner, it is seen that security explore is far from produce for the recently risen CPS and there are up till now numerous challenges defying creators, administrators and scientists.

(Edward, 2015), battled that deterministic models have genuinely shown to an incredible degree supportive and even shape the unrivalled, of the modern upset and the computerized and data innovation transformations. Key deterministic models join differential conditions, synchronous advanced rationale, single-strung basic projects and guidance set structures. CPS, regardless, unite these models with the end goal that determinism isn't protected. Two tasks were depicted showing that deterministic CPS models with dependable physical acknowledge are possible and convenient. The main task is PRET, which exhibits that the planning accuracy of synchronous computerized rationale can be for all intents and purposes made accessible at the product level of reflection. The second endeavour is Ptides, which shows that deterministic models for dispersed CPS have useful devoted acknowledge. Ptides use organize clock synchronization, which is accept to end up omnipresent. These tasks are insignificant presence proofs, and there is apparently that more work is required before specialists routinely use deterministic models for CPS. In end it was guessed that a nice deterministic displaying worldview for CPS will fuel the following innovation upset.

(Xi and Christine, 2015), examined the check and approval in CPSs. Watching out for the insufficiency of observational data available about CPS enhancement, especially in investigating and testing. An observational examination with three areas was coordinated: a wide writing audit, a quantitative on-line review, and subjective meetings. In the written works investigated, an exceptionally wide take a gander at methods that have been or could be associated with CPS confirmation and approval was finished.

The Brace design, which fits these parts together. CPS architects use an affirmation dialect to comment on a CPS program with wanted accuracy ensures. This clarified program is gone through the Brace compiler to the runtime system, which uses an arrangement of devices that model and connect with the physical parts of a CPS to deliver a deployable CPS program. BraceForce alludes to a device that offers access to physical information from sensors and actuators sent in nature. BraceBind alludes to a device that relates the engineer's accuracy particulars either to yields of these sensors and actuators or to models of physical properties.

This strawman engineering clarifies explore difficulties in passing on reasonable runtime confirmation to CPS improvement. At first, decide dialect for naturally and expressively expressing CPS declarations; this is BraceAssertion. Moreover, the cutting edge in runtime check does not have a concordance among expressiveness and productivity. Furthermore, CPS has obvious necessities for runtime check. Prop is a web-based checking structure that address these issues. Thirdly, as found in the experimental investigations, physical properties can't be simply neglected, and a solid method to manage speaking to the intertwined physical and digital parts of a CPS must be kept an eye on; this is BraceBind. At last, CPS show stochastic attributes: sensors can be inadequate, deferrals of activation are arbitrary, and effects of the sending condition are frequently undetermined. In light of the results, the runtime check, hand crafted to the one of a kind needs of CPS offers a sensible and achievable enhancement to existing experimentation testing approaches in CPS, where designers are currently tuned to recognizing and possibly responding to inadequacies dynamically.

(Amit, 2016), highlighted a couple of chances and challenges for improving Cyber security in CPSs as pursues: Layered Defense: The essential layer of digital security fuses firewalls and the parcel of unmistakable systems. The second layer of digital security joins discovery of endeavours and conventional reactions to them. The third layer of digital security consolidates infection scanners and email channels. Malware Detection: Using mindfulness about using safe web, to keep customers from genuine malware assaults. A PC physical framework must recognize both known and obscure infections and spam. Hence, a program section or tad of data from a greater set can be used as a discovery layout. This removed data can be stood out from correspondingly removed data from an infection/spam. The latter is known as the "signature" of the infection/spam. The present CPS need to give some insurance to malware and spam in light of the fact that the on-going proximity of significant volumes of spam and malware, and abuses, suggests that the present assurances are unnecessarily limited in their abilities and requires more imperative respect for the norms of security as inserted in PC framework tasks which would offer climb to upgraded results.

(Henry, Mohammad, and Danny, 2016), gotten to condition of-workmanship ways to deal with handle self-adjustment in CPS at the building level. An exact composition study was driven by means of looking for four noteworthy logical information bases, achieving 1103 confident examinations and unavoidably holding 42 essential investigations included for information gathering in the wake of applying incorporation and rejection criteria.

The fundamental stresses of adjustment in CPS are execution, adaptability, and unwavering quality. 64% of the examinations apply adjustment at the application layer and 24% at the middleware layer. MAPE (Monitor-Analyze-Plan-Execute) is the predominant adjustment system (60%), trailed by specialists and self-association (both 29%). Astoundingly, 36% of the examinations combine unmistakable frameworks to acknowledge adjustment; 17% unite MAPE with operators. The mind-boggling application space is vitality (24%). This raises difficulties for future research both in the field of CPS and self-adjustment, including: how to delineate to layers and adjustment components, how to facilitate adjustment instruments inside and crosswise over layers, and how to guarantee framework wide consistency of adjustment.

(Abdulmalik, Jingqiang, Fengjun, and Bo, 2017), checked on composed deals with security and protection of CPS, with an outstanding focus on four agent CPS applications: Information Computing System, keen frameworks, medicinal gadgets, and shrewd autos. A digital physical security structure that wires CPS angles into the security points of view. The framework catches how a strike of the physical space of a CPS can realize unanticipated results in the digital area and the other way around close by proposed arrangements. Using this structure, successful controls can be made to dispose of digital physical assaults. For example, it was recognized that the heterogeneity of CPS parts contributes out and out to numerous ambushes. Along these lines, a viable arrangement should give watchful thought when heterogeneous segments communicate.

(Hussain, Long, Danfeng, and Homa, 2017), focused their examination on a serious understanding of risk demonstrating in Medical CPS. What's more, left on promising best in class inquire about patterns for keeping an eye on Medical CPS security concerns. Right off the bat, Anomaly Detection: Runtime seeing of Medical CPS is a fruitful countermeasure against various assaults. The dominant part of existing works in this field are conduct display based, which can be moreover divided into two: Physics-based models describing ordinary activities in CPS for oddity identification, where framework states must take in the wake of perpetual laws of material science in CPS. And digital-based models depicting the normal program/framework practices to see potential assaults. Also, Cryptographic Measures: cryptography is a generally used methodology for anchoring the correspondence channel from unapproved get to. Nevertheless, dominant part of the ordinary cryptographic natives that have been used when all is said in done reason IT frameworks, both figure and hash capacities, can't be particularly associated with Medical CPS as a result of the size, continuous, and control requirements of medicinal gadgets. Thirdly, System Hardening: Secure execution condition can be used to protect a broad assortment of dangers in Medical CPS. Restricting security-basic applications from untrusted OS is a promising strategy to enhance Medical CPS security.

III. CPS SECURITY OBJECTIVE

In ensuring CPS security, various objectives are to be achieved. The objectives (6) and their associated references: confidentiality, integrity, availability, robustness, reliability and trustworthiness (Acatech, 2011) are shown below:

1. **Confidentiality:** Confidentiality means that prevention of unapproved revelation of information would be handled by the CPS
2. **Integrity:** Integrity refers to data or resources cannot be modified without authorization. Ensuring data integrity necessitates the power to discover any changes introduced (maliciously or otherwise) in the message being communicated.
3. **Availability:** High availability of cyber physical system aims to always provide service by preventing computing, controls, communication corruptions due to hardware failures, system upgrades, power outages or denial-of-service attacks.
4. **Reliability:** An unreliable CPS mostly causes system defect, service disturbances, financial losses and loss of human life.
5. **Robustness:** Robustness means despite disruptions; a system is able to perform accurately to a standard i.e. notwithstanding erroneous inputs.
6. **Trustworthy:** Trustworthiness of CPS means under certain functional and atmospheric conditions, how correctly a system would function carrying out the tasks solely in a reliable manner over a certain period of time or at any given instance.

IV. Security Control and Attacks in CPS

4.1 Attacks in CPS: Different kinds of attacks have been mentioned by (Piyush, 2016) and (Derui, Qing-Long, Yang, Xiaohua, & Xian-Ming, 2017). The different kinds of attacks are summarized as follows:

1. **Eavesdropping:** Eavesdropping in CPS refers that attacker, rather than involving himself directly with the functioning of CPS; witnesses the activities and hitherto utilizes the information to violate users' privacy and/or security.
2. **Denial of service attack:** This is a type of onslaught to make the system resources inaccessible. From the innovation perspective,

attackers can fill buffers of user domains or kernel domains, gridlock the shared network medium to prevent devices gadgets from conveying or accepting, or change the routing protocol.

3. **Stealthy Deception attack:** This is a kind of attack, in which the information trustworthiness is adjusted for transmitted packets among different cyber-parts. For example, Stuxnet worms can reprogram the code running in programmable logic controllers (PLCs) in Supervisory Control and Data Acquisition (SCADA) systems such that the systems diverge from their expected activities.
4. **Replay attacks:** This attack is a raw mode in which a legitimate information is deceitfully iterated or held up tactically. An assumed attack is thought to fake the length among the nodes by interrupting the routing protocol.
5. **Compromised-Key attack:** In such kind of attack the hacker would try to penetrate the secure resource so as to create extra keys which have been altered by either decrypting or modifying information.

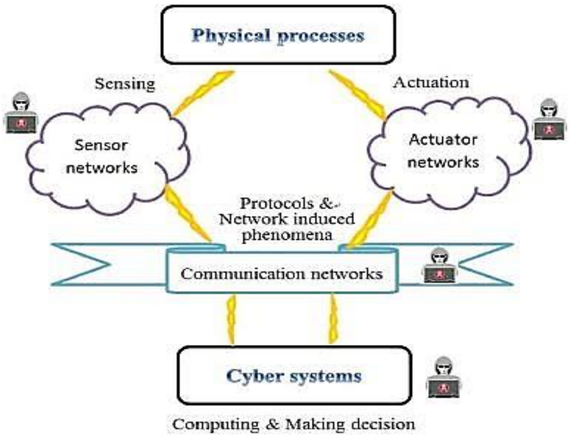

Figure 3 : Security Control and Attack Detection for Industrial Cyber-Physical System

Source: (Derui, Qing-Long, Yang, Xiaohua, & Xian-Ming, 2017)

4.2 Security Control

1. Power Network Security: The present electric grid is a large scale, computer-mediated physical distributed complex arrangement of systems, on which CPS remain to have a huge effect. With the combination of cutting-edge computing and communication advances, the smart grid is required to enormously upgrade productivity and distributed intelligence (Wang & Lu, 2013). The smart grid carries with its numerous new information accumulation, communication, and data sharing limits in the power system alongside new security dangers, vulnerabilities and related cyber-physical attacks.

2. Medical CPS Security: Medical digital physical frameworks are life-basic, setting mindful, sorted out frameworks of medical gadgets. The earlier decades have seen an imaginative distress in human services field. New materials displace metals and gadgets and frameworks in light of information data innovation replacing straightforward gadgets to be used as a piece of determining diagnosis, observing, and treatment. Computing, detecting, displaying, and communication progress over the years significantly organized in physical parts allow medicinal digital physical frameworks to achieve new levels of execution with unprecedented value (NIST, 2013). Interoperable therapeutic gadgets, in light of its systems administration and coordination functionalities and extended assault surface, stand up to perils of frameworks security.

3. Smart Manufacturing Security : Smart manufacturing joins development, learning, information, and human imagination to make and apply "manufacturing information" (NIST, 2013). Savvy production considers the aggregate enhancement of an assembling plant, where information can be conferred among mechanical machines consistently. As development progresses, digital physical frameworks are getting the chance to be clearly defenceless against a broader extent of assaults. In assembling, these assaults constitute a basic hazard to ensuring items fit in with their one of a kind layout plans and to keeping up the security of hardware, workers, and customers.

V. Cyber-Physical System in Different Sectors

Some of the various economic sectors where CPS has found its growth are discussed below:

1. **CPS in Power Network:** CPS are vital to interior obligations to lessen energy utilized while expanding performance, dependability, and efficiency across economic sectors—via the smart grid, smart transportation systems, smart manufacturing, and smart buildings infrastructure (Janos, et al., 2013). The electric power transmission grid, shapes one of the biggest complex interconnected systems at any point fabricated. Under ordinary operation, this web of interconnecting transmission lines makes the grid exceptionally strong and dependable. New arrangements including advanced power electronics and energy stockpiling are accessible, however coordination and investigation of associations of these assets remains an open research challenge (Ragunathan, Insup, Lui, & John, 2010). Clean renewable electric energy assets, for example, solar and wind and innovative items, for example, electric vehicles are required to progress altogether, particularly as costs descend. The combination of irregular and uncertain wind and sun-oriented sources and module devices requires new sensors, switches and meters, as well as a smart infrastructure for understanding a smart grid - a versatile, strong, productive, and financially savvy power dispersion system. CPS innovations are basic for the production of this infrastructure, empowering the streamlining and administration of resources and facilities, enabling consumers to control and deal with their energy utilization (PCAST P. C., 2011).

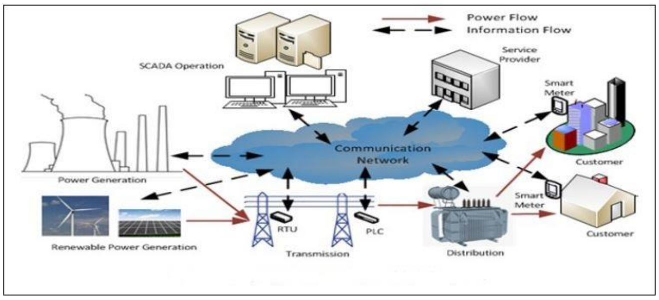

Figure 4 : Smart Grid Cyber-Physical Systems
Source: (Mohammad, Mohammed, Dipankar, Robert, & Shubhalaxmi, 2015)

2. **CPS in Medicine:** CPS is as of now encouraging a wide move from clinic based to home-based health care. By broadening the span of quality care past conventional doctor's facilities, CPS-based medical devices and system are empowering more personalized health care services and amended patient results. As progress made are influenced, CPS can prompt new capacities to diagnose, treat, and forestall infection. CPS counts on detecting, preparing, and organizing. The current progress in wireless sensor networks (WSN), medical sensors, and Cloud Computing are making CPS an intense contender for medicinal services applications including in-hospital and in-home patient care (Janos, et al., 2013). These progressions guarantee to give CPS the capability to watch patient vitals at a distance and making contributions paying little mind to the patient's whereabouts. These sensors can gather key patient data containing wellbeing information. Gathered information are sent to a portal by means of the wireless communication medium. Wired sensors can likewise be utilized; in any case, sensors give greater adaptability and solace to both the caregiver and the patients. The information gathered by the sensors can be put away in a server and made available to clinicians. Security

is an essential worry here as patient information is secret from legal and ethical points of view. Along these lines, while designing CPS architecture for medicinal services applications, unique considerations should be paid to guarantee information security (Shah, Syed, & Mustafizur, 2014).

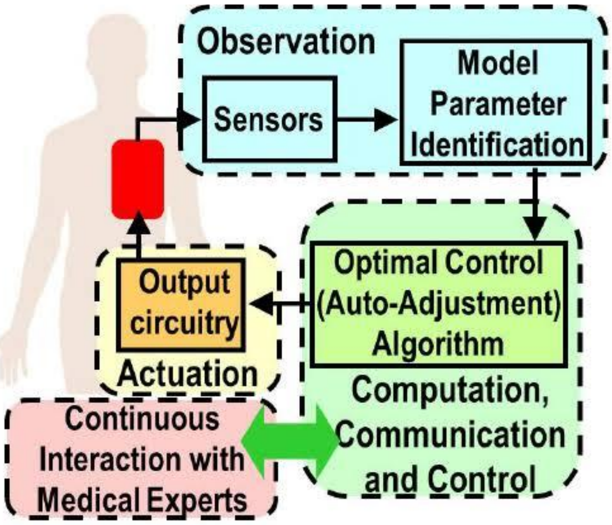
Observation
Sensors
Model Parameter Identification
Optimal Control (Auto-Adjustment) Algorithm
Output circuitry
Actuation
Computation, Communication and Control
Continuous Interaction with Medical Experts

Figure 5 : CPS Approach to Pacemaker Design
Source: (Paul, Siddhartha, & Radu, 2013)

3. **CPS in Manufacturing:** CPSs are additionally of real relevance in mechanical generation, keeping in mind the end goal to have the capacity to execute customer necessities. In-house creation procedures can be upgraded, prompting enhancements in the environmental accounting report. Production systems will be set up that can respond for all intents and purposes continuously to changes in the market and the inventory network utilizing CPSs, and which collaborate with ultra-adaptability even past organization limits (Acatech, 2011). The unpredictability of what we can design and construct, and what society (and military) needs is always expanding, while the time scale for products and the lead time are diminishing, even as product assortment is expanding. CPS advances are fundamental to protecting our national aggressiveness in manufacturing and for national security. The "joining of the worldwide modern industrial system with the power of advanced computing, analytics, low-cost sensing, and new levels of availability allowed by the Internet" has likewise been known as the Industrial Internet.

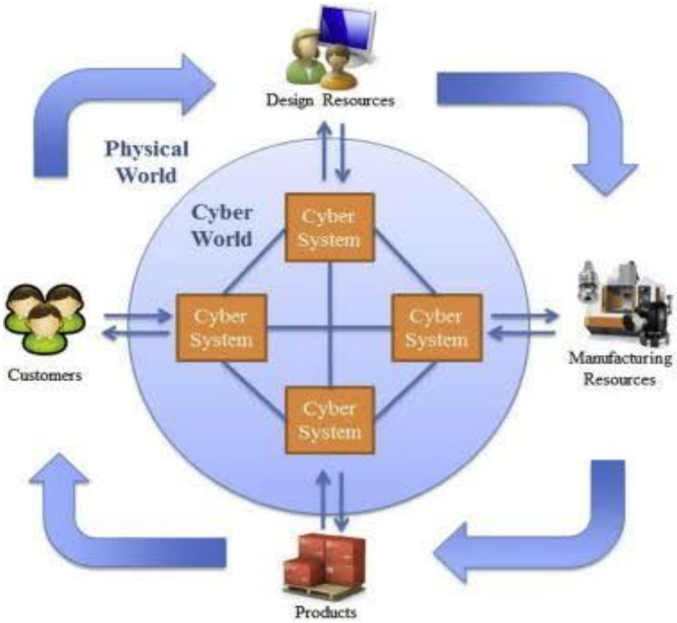

Figure 6 : Manufacturing Cyber-Physical Systems
Source: (Chunyang, Xun, & Yuqian, 2015)

VI. CONCLUSION

Great development has been made in the enhancement of CPS, anyway numerous challenges flourish. Beating these challenges makes stimulating developmental opportunities to ensure that diverse money related divisions in the field of CPS, will have a globally forceful edge. The ability of CPS to change each piece of life is gigantic. Thoughts in various parts have been produced, setting it in the cutting edge of mechanical progression. These frameworks all rely upon a computational center that is solidly interconnected with parts in the physical world; putting out each day practices both at home and work promptly accessible.

The essential particular challenges in like manner have a great deal of shared attribute reflecting an extent of central logical, designing, institutional, and societal issues. Hindrances rise all through all periods of development headway, from principal science through connected Research and Development, show, assembling, and organization. Keeping an eye on the most belittling of these will help ensure that, the future CPS are solid, protected, producible, and secure.

VII. REFERENCES

[1]. Abdulmalik, H., Jingqiang, L., Fengjun, L., & Bo, L. (2017). Cyber-Physical Systems Security - A Survey. 1-28.

[2]. Acatech. (2011). Cyber-Physical Systems. acatech POSITION PAPER.

[3]. Amit, K. T. (2016, March). Cyber Physical Systems (CPSs) - Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications, 137(14), 19-27.

[4]. Chunyang, Y., Xun, X., & Yuqian, L. (2015). Computer-Integrated Manufacturing, Cyber-Physical Systems and Cloud Manufacturing - Concepts and Relationships. ScienceDirect, 6, 5-9. doi:10.1016/j.mfglet.2015.11.005

[5]. Derui, D., Qing-Long, H., Yang, X., Xiaohua, G., & Xian-Ming, Z. (2017). A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 1674-1683.

[6]. Edward, A. L. (2015). The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. Sensors, 4837-4869. doi:10.3390/s150304837

[7]. Erik, W.-S. (2018). Cyber Physical Systems (CPS). Retrieved from IoT ONE: https://m.iotone.com/term/cyber-physical-system-cps/t145

[8]. Henry, M., Mohammad, S., & Danny, W. (2016). Self-Adaptation for Cyber-Physical Systems: A Systematic Literature Review. ACM, 1-7. doi:10.1145/1235

[9]. Hussain, A., Long, C., Danfeng, D. Y., & Homa, A. (2017). On Threat Modeling and Mitigation of Medical Cyber-Physical Systems. 1-6.

[10]. Insup, L., Oleg, S., Sanjian, C., John, H., Eunkyoung, J., BaekGyu, K., . . . Krishna, V. (2012). Challenges and Research Directions in Medical Cyber-Physical Systems. IEEE, 75-90. Retrieved from http://dx.doi.org/10.1109/JPROC.2011.2165270

[11]. Janos, S., Susan, Y., Isaac, C., David, C., Jim, D., Himanshu, K., . . . Lonny, S. (2013). Foundations for Innovation: Strategic R&D Opportunities for 21st Century Cyber-Physical Systems. National Institute of Standards and Technology. Retrieved from http://events.energetics.com/NIST-CPSWorkshop/downloads.html

[12]. Jay, C. (2018, August 31). Industry 4.0: Impact of Digitalization on Finance and Accountancy. Retrieved from Accountancy Resourcing Group: www.accountancyresourcinggroup.co.uk/news-and-insights/industry-40-impact-of-digitalization-on-finance-and-accountancy/

[13]. Mohammad, A. H., Mohammed, H. A., Dipankar, D., Robert, K. A., & Shubhalaxmi, K. (2015). Co-Simulation Platform For Characterizing Cyber Attacks in Cyber Physical Systems. 2015 IEEE Symposium Series on Computational Intelligence (pp. 1244-1251). IEEE. doi:10.1109/SSCI.2015.178

[14]. NIST, N. I. (2013). Foundations for Innovation in Cyber-Physical Systems Workshop Summary Report". National Institute of Science and Technology. Retrieved from http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf.

[15]. Paul, B., Siddhartha, J., & Radu, M. (2013). Pacemaker Control of Heart Rate Variability: A CPS perspective. ACM.

[16]. PCAST, P. C. (2007). Leadership Under Challenge: Information Technology R&D in a Competitive World.

[17]. PCAST, P. C. (2011). Ensuring American Leadership in Manufacturing.

[18]. Piyush, M. (2016). Security Issues of Cyber Physical System: A Review. International Journal of Computer Applications, 7-11.

[19]. Ragunathan, R., Insup, L., Lui, S., & John, S. (2010). Cyber-Physical Systems: The Next Computing Revolution. Design Automation Conference (pp. 1-6). Anaheim, California, USA: ACM.

[20]. Shah, A. H., Syed, M. A., & Mustafizur, R. (2014). Review of Cyber-Physical System in Healthcare. International Journal of Distributed Sensor Networks, 1-21. Retrieved from http://dx.doi.org/10.1155/2014/217415

[21]. Shailesh, K. J. (2014). Medical Cyber Physical System. International Journal of Emerging Technology and Advanced Engineering, 4(5), 1-5.

[22]. Tianbo, L., Jinyang, Z., Lingling, Z., Yang, L., & Xiaoyan, Z. (2015). Towards a Framework for Assuring Cyber Physical System Security. International Journal of Security and Its Applications, 9(3), 25-40. Retrieved from http://dx.doi.org/10.14257/ijsia.2015.9.3.04

[23]. Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5), 1344-1371.

[24]. Xi, Z., & Christine, J. (2015). Verification and Validation in Cyber Physical Systems: Research Challenges and a Way Forward. 1-4.